H/wk 10, Solutions to selected problems

Ch. 2.10, Problem 18

If $G = H \times K$ and $K_1 = \{(1,k)|k \in K\}$, show that $K_1 \lhd G$, $K_1 \cong K$ and $G/K_1 \cong H$.

Solution.

Consider the function $f : G \to H$ defined as $f(h,k) = h$ for $h \in H, k \in K$. We claim that f is an onto homomorphism and that $K_1 = Ker(f)$. It is obvious that the function f is onto. To see that f is a homomorphism, note that

$$f\big((h,k)(h_1,k_1)\big) = f(hh_1,kk_1) = hh_1 = f(h,k)f(h_1,k_1).$$

Thus indeed f is a homomorphism. We also have

$$Ker(f) = \{(h,k) \in H\times K|f(h,k) = 1\} = (h,k) \in H\times K|h = 1\} = \{(1,k)|k \in K\} = K_1.$$

Thus $Ker(f) = K_1$ which implies that $K_1 \lhd G$. Moreover, since $f : G \to H$ is onto, the Isomorphism Theorem implies that $G/K_1 = G/Ker(f) \cong H$.

It remains to show that $K_1 \cong K$. Consider the function $\alpha : K \to K_1$ defined by $\alpha(k) = (1,k)$ for $k \in K$. It is obvious that α is a bijection. We also have

$$\alpha(kk_1) = (1,kk_1) = (1,k)(1,k_1) = \alpha(k)\alpha(k_1).$$

Thus α is a homomorphism. Therefore $\alpha : K \to K_1$ is an isomorphism and $K_1 \cong K$, as required. $\Box$

Ch. 2.10, Problem 21

Show that $\mathbb{C}^*/\mathbb{C}^0 \cong \mathbb{R}^+$ where $\mathbb{C}^0 = \{z \in \mathbb{C} : |z| = 1\}$ is the circle group.

Solution.

Recall that $\mathbb{C}^* = \mathbb{C} - \{0\}$ and $\mathbb{R}^+ = (0,\infty)$. Consider the function

$$f : \mathbb{C}^* \to \mathbb{R}^+, \quad f(z) = |z|, \quad z \in \mathbb{C}^*.$$

We claim that f is a group homomorohism. Indeed

$$f(z_1z_1) = |z_1z_2| = |z_1|\ |z_2| = f(z_1)f(z_2).$$

Thus indeed f is a homomorphism. The function f is easily seen to be onto. Indeed, for any $r \in \mathbb{R}^+$ we have $|r| = r$ and thus $f(r) = r$.

We next compute the kernel of f:

$$Ker(f) = \{z \in \mathbb{C}^* : f(z) = 1\} = \{z \in \mathbb{C}^* : |z| = 1\} = \mathbb{C}^0.$$

Thus $Ker(f) = \mathbb{C}^0$. Since $f : \mathbb{C}^* \to \mathbb{R}^+$ is an onto homomorphism and $Ker(f) = \mathbb{C}^0$, the Isomorphism Theorem now implies that $\mathbb{C}^*/\mathbb{C}^0 \cong \mathbb{R}^+$, as required. $\Box$

Ch. 3.1, Problem 13

If $u, v, (u+v)$ are units in a ring R, show that $u^{-1} + v^{-1}$ is also a unit and give a formula for $(u^{-1} + v^{-1})^{-1}$ in terms of u, v and $(u+v)^{-1}$.

Solution.

We have

$$u(u^{-1} + v^{-1})v = (1 + uv^{-1})v = v + u = u + v.$$

Therefore

$$u^{-1} + v^{-1} = u^{-1}(u+v)v^{-1}$$

is a product of three units. Hence $u^{-1}+v^{-1}$ is also a unit and

$$(u^{-1}+v^{-1})^{-1} = (v^{-1})^{-1}(u+v)^{-1}(u^{-1})^{-1} = v(u+v)^{-1}u. \quad \square$$

Ch. 3.1, Problem 14

Given r and s in a ring R, show that $1+rs$ is a unit if and only if $1+sr$ is a unit.

Solution.

Note that $s(1+rs) = s+srs = (1+sr)s$ and, similarly, $(1+rs)r = r+rsr = r(1+sr)$.

Suppose that $1+rs$ is a unit. Put $x := 1-s(1+rs)^{-1}r$. We claim that x is the inverse of $1+sr$ in R. Indeed, we have

$$(1+sr)x = (1+sr)[1-s(1+rs)^{-1}r] = 1+sr-(1+sr)s(1+rs)^{-1}r =$$
$$1+sr-s(1+rs)(1+rs)^{-1}r = 1+sr-sr = 1$$

and

$$x(1+sr) = [1-s(1+rs)^{-1}r](1+sr) = 1+sr-s(1+rs)^{-1}r(1+sr) =$$
$$1+sr-s(1+rs)^{-1}(1+rs)r = 1+sr-sr = 1.$$

Thus $(1+sr)x = x(1+sr) = 1$ and hence $1+sr$ is a unit.

This shows that if $1+rs$ is a unit then $1+sr$ is a unit, as required.

Ch. 3.1, Problem 18. In each case find the characteristic of the ring:

(a) $\mathbb{Z}_n \times \mathbb{Z}_m$;
(b) $M_2(\mathbb{Z}_n)$.
(c) $\mathbb{Z} \times \mathbb{Z}_m$

Answers:

(a) $char(\mathbb{Z}_n \times \mathbb{Z}_m) = lcm(n,m)$;
(b) $char(M_2(\mathbb{Z}_n)) = n$.
(c) $char(\mathbb{Z} \times \mathbb{Z}_m) = 0$.

Ch 3.1, Problem 33

A ring R is called **Boolean** if $r^2 = r$ for every $r \in R$. Show that every boolean ring $R \neq 0$ is commetative of characteristic 2.

Solution.

For every $r \in R$ we have

$$r+1 = (r+1)^2 = r^2+2r+1 = r+2r+1 = 3r+1 \quad \Longrightarrow \quad 2r = 0.$$

Thus for every $r \in R$ we have $2r = 0$. Since $R \neq 0$, this implies that $char(R) = 2$.

Note that since $char(R) = 2$, we have $2r = 0$, that is $r = -r$ for every $r \in R$.

Let $a, b \in R$ be arbitrary. Then

$$a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b \Longrightarrow \quad ab+ba = 0.$$

Hence $ba = -ab$ for every $a, b \in R$. Since $r = -r$ for every $r \in R$, we have $-ab = ab$ and hence $ba = ab$ for every $a, b \in R$. Thus R is commutative, as required.